# AnyConnect FAQ: Los túneles, vuelven a conectar el comportamiento, y el temporizador de inactividad

## Contenido

# Introducción

Este documento describe detalladamente algunos puntos importantes sobre los túneles del Cliente de movilidad Cisco AnyConnect Secure (AnyConnect), el comportamiento del volver a conectar y el Dead Peer Detection (DPD), y el temporizador de inactividad.

# Antecedentes

## Tipos de túneles

Hay dos métodos usados para conectar una sesión de AnyConnect:

- Vía el porta (clientless)
- Vía la aplicación autónoma

De acuerdo con la manera usted conecta, usted crea tres diversos túneles (sesiones) en el ASA, cada uno con un propósito específico:

1. **Clientless o Padre-túnel:** Ésta es la sesión principal que se crea en la negociación para configurar el token de la sesión que es necesario en caso de que un volver a conectar sea necesario debido a los problemas de conectividad de red o a la hibernación. De acuerdo con el mecanismo de conexión, el dispositivo de seguridad adaptante de Cisco (ASA) enumera la sesión como el clientless (Weblaunch vía el portal) o padre (AnyConnect independiente).

   Nota: El AnyConnect-padre representa la sesión cuando el cliente no está conectado activamente. Con eficacia, trabaja similar a un Cookie, en que es una entrada de la base de datos en el ASA ese asocia a la conexión de un cliente particular. Si el cliente apaga o los sueños, los túneles (IPSec/Internet Key Exchange (IKE)/los protocolos del Transport Layer Security del Transport Layer Security (TLS) /Datagram (DTL)) se rasgan abajo, solamente los restos del padre hasta el tiempo de conexión del temporizador de inactividad o del máximo toman el efecto. Esto permite que el usuario vuelva a conectar sin reauthenticating.

2. **Secure Sockets Layer (SSL) - Túnel:** La conexión SSL se establece primero, y los datos se pasan sobre esta conexión mientras que intentan establecer una conexión DTL. Una vez que se establece la conexión DTL, el cliente envía los paquetes vía la conexión DTL en vez vía de la conexión SSL. Los paquetes de control, por otra parte, pasan siempre la conexión SSL.

3. **DTL-túnel:** Cuando el DTL-túnel se establece completamente, todos los datos se mueven al DTL-túnel, y el SSL-túnel se utiliza solamente para el tráfico ocasional del canal de control.

Si algo sucede al User Datagram Protocol (UDP), el DTL-túnel se derriba y todos los pasos de los datos a través del SSL-túnel otra vez.

## Salida de muestra del ASA

Aquí está la salida de muestra de los dos métodos de conexión.

## AnyConnect conectó vía el Red-lanzamiento:

```
ASA5520-C(config)# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : walter Index : 1435
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Protocol : Clientless SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : Clientless: (1)RC4 SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing : Clientless: (1)SHA1 SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 335765 Bytes Rx : 31508
Pkts Tx : 214 Pkts Rx : 18
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : My-Network Tunnel Group : My-Network
Login Time : 22:13:37 UTC Fri Nov 30 2012
Duration : 0h:00m:34s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none

Clientless Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

Clientless:
Tunnel ID : 1435.1
Public IP : 172.16.250.17
Encryption : RC4 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : Web Browser
Client Ver : Mozilla/5.0 (Windows NT 5.1; rv:16.0) Gecko/20100101 Firefox/16.0
Bytes Tx : 329671 Bytes Rx : 31508

SSL-Tunnel:
Tunnel ID : 1435.2
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Encryption : RC4 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Src Port : 1241
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.01065
Bytes Tx : 6094 Bytes Rx : 0
Pkts Tx : 4 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 1435.3
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Encryption : AES128 Hashing : SHA1
```

```
Encapsulation: DTLSv1.0 Compression : LZS
UDP Src Port : 1250 UDP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : DTLS VPN Client
Client Ver : Mozilla/5.0 (Windows NT 5.1; rv:16.0) Gecko/20100101 Firefox/16.0
Bytes Tx : 0 Bytes Rx : 0
Pkts Tx : 0 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

## AnyConnect conectó vía la aplicación autónoma:

```
ASA5520-C(config)# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : walter Index : 1436
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 12244 Bytes Rx : 777
Pkts Tx : 8 Pkts Rx : 1
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : My-Network Tunnel Group : My-Network
Login Time : 22:15:24 UTC Fri Nov 30 2012
Duration : 0h:00m:11s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
Tunnel ID : 1436.1
Public IP : 172.16.250.17
Encryption : none Hashing : none
TCP Src Port : 1269 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : AnyConnect
Client Ver : 3.1.01065
Bytes Tx : 6122 Bytes Rx : 777
Pkts Tx : 4 Pkts Rx : 1
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 1436.2
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Encryption : RC4 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Src Port : 1272
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.01065
Bytes Tx : 6122 Bytes Rx : 0
Pkts Tx : 4 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 1436.3
```

```
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Encryption : AES128 Hashing : SHA1
Encapsulation: DTLSv1.0 Compression : LZS
UDP Src Port : 1280 UDP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : DTLS VPN Client
Client Ver : 3.1.01065
Bytes Tx : 0 Bytes Rx : 0
Pkts Tx : 0 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

# DPD y temporizadores de inactividad

## ¿Cuándo una sesión se considera una sesión inactiva?

La sesión se considera inactiva (y el temporizador comienza a aumentar) solamente cuando el SSL-túnel no existe más en la sesión. Así pues, cada sesión es con impresión horaria con el tiempo de descenso del SSL-túnel.

```
ASA5520-C# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : walter Index : 1336
Public IP : 172.16.250.17
Protocol : AnyConnect-Parent    <- Here just the AnyConnect-Parent is active
but not SSL-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none
Hashing : AnyConnect-Parent: (1)none
Bytes Tx : 12917 Bytes Rx : 1187
Pkts Tx : 14 Pkts Rx : 7
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : My-Network Tunnel Group : My-Network
Login Time : 17:42:56 UTC Sat Nov 17 2012
Duration : 0h:09m:14s
Inactivity   : 0h:01m:06s           <- So the session is considered Inactive
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
```

## ¿Cuándo el ASA cae el SSL-túnel?

Hay dos maneras que un SSL-túnel puede ser disconnected:

1. DPD - Los DPD son utilizados por el cliente para detectar un error en las comunicaciones entre el cliente de AnyConnect y el centro distribuidor ASA. Los DPD también se utilizan para limpiar los recursos en el ASA. Esto se asegura de que el centro distribuidor no mantenga las conexiones la base de datos si el punto final es no sensible a los ping DPD. Si el ASA envía un DPD al punto final y responde, no se toma ningunas medidas. Si el punto final no es responsivo, el ASA derriba el túnel en la base de datos de la sesión, y se traslada la sesión a “esperar para reanudar” el modo. Cuál este los medios son que el DPD del centro distribuidor ha comenzado, y el centro distribuidor comunica no más con el cliente. En tales situaciones, el ASA detiene el Padre-túnel para permitir que el usuario vague por las

redes, vaya a dormir, y recupere la sesión. Estas sesiones cuentan contra las sesiones activo-conectadas y se borran bajo estas condiciones:
Ocioso-descanso del usuarioEl cliente reanuda a la sesión original y termina la sesión correctamente
Para configurar los DPD, utilice el comando del DPD-intervalo del anyconnect bajo atributos del WebVPN en las configuraciones de la grupo-directiva. Por abandono, el DPD se habilita y se fija a 30 segundos para el ASA (gateway) y el cliente.

Precaución: Sea consciente del Id. de bug Cisco CSCts66926 - El DPD no puede terminar los DTL hace un túnel después de la conexión cliente perdida.

2. **Ocioso-descanso** - La segunda manera que el SSL-túnel es disconnected es cuando expira el Ocioso-descanso para este túnel. Sin embargo, recuerde que es no sólo el SSL-túnel que debe estar desocupado hacia fuera, pero los DTL hacen un túnel también. A menos que los tiempos de la sesión DTL hacia fuera, el SSL-túnel se conserve en la base de datos.

### ¿Por qué el Keepalives necesita ser habilitado si los DPD se habilitan ya?

Según lo explicado previamente, el DPD no mata a la sesión sí mismo de AnyConnect. Mata simplemente al túnel dentro de esa sesión de modo que el cliente pueda restablecer el túnel. Si el cliente no puede restablecer el túnel, sigue habiendo la sesión hasta que el temporizador de inactividad expire en el ASA. Puesto que los DPD se habilitan por abandono, los clientes pudieron conseguir a menudo disconnected debido a los flujos que se cerraban en una dirección con los dispositivos del Network Address Translation (NAT), del Firewall y del proxy. Habilitar el Keepalives en los intervalos bajos, tales como 20 segundos, ayuda a prevenir esto.

El Keepalives se habilita bajo atributos del WebVPN de una grupo-directiva determinada con el comando keepalive SSL del anyconnect. Por abandono, los temporizadores se fijan a 20 segundos.

## El comportamiento del cliente de AnyConnect en caso de vuelve a conectar

AnyConnect intentará volver a conectar si se interrumpe la conexión. Esto no es configurable, automáticamente. Mientras la sesión de VPN en el ASA sea todavía válida y si AnyConnect puede restablecer la conexión física, reanudarán a la sesión de VPN.

La característica del volver a conectar continúa hasta el tiempo de espera de la sesión o el descanso de la desconexión, que es realmente el tiempo de inactividad, expira (o 30 minutos si no se configura ningunos descansos). Una vez que expiran éstos, usted no debe continuar porque el ASA habrá caído a la sesión de VPN. El cliente continuará mientras piense que el ASA todavía tiene la sesión de VPN.

AnyConnect volverá a conectar no importa cómo la interfaz de la red cambia. No importa si la dirección IP de los cambios del Network Interface Cards (NIC), o si Switches de la Conectividad a partir de un NIC a otro NIC (Tecnología inalámbrica a atado con alambre o vice versa).

Cuando usted considera el proceso del volver a conectar para AnyConnect, hay tres niveles de

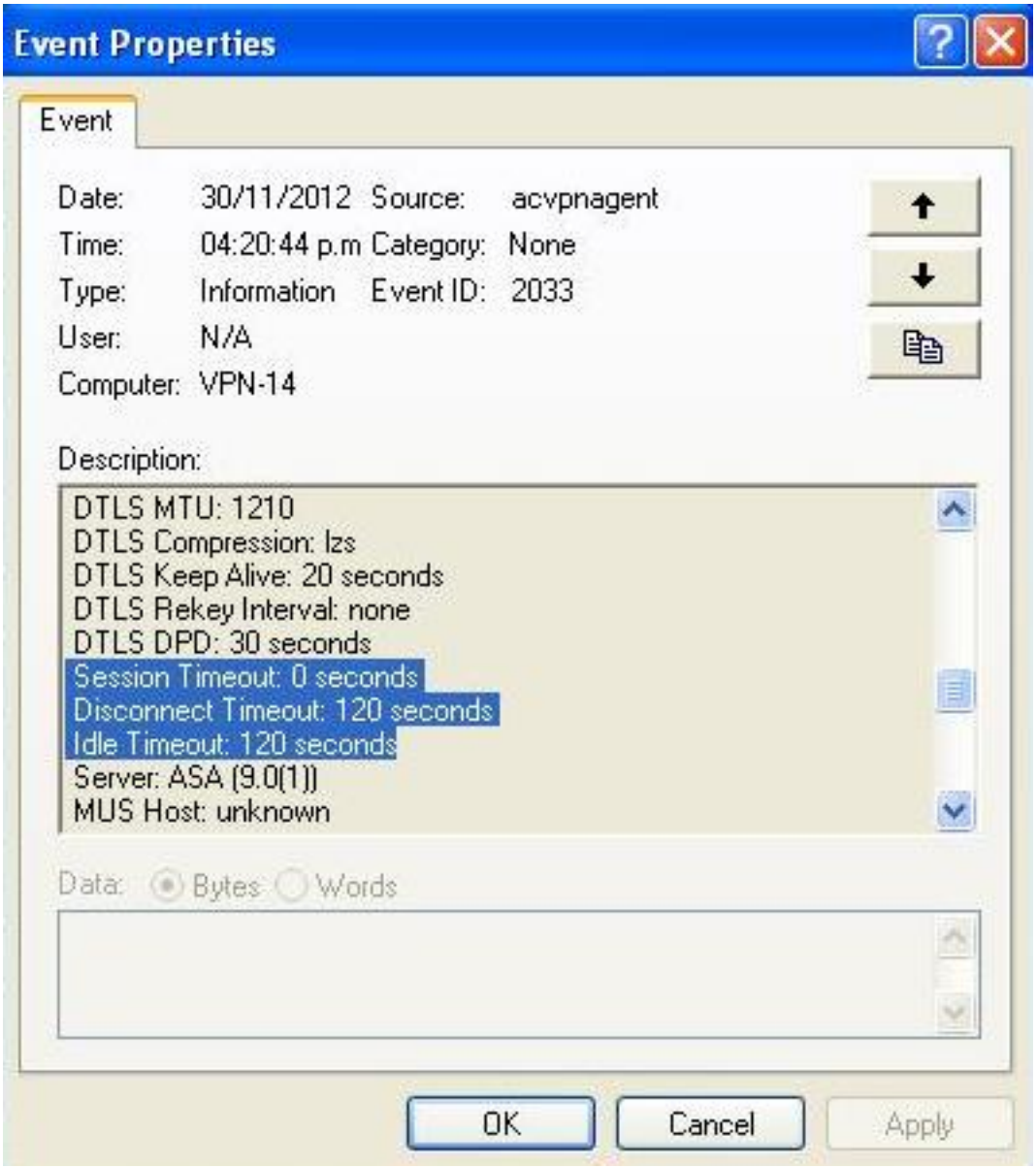
sesiones que usted deba recordar. Además, el comportamiento del volver a conectar de cada uno de estas sesiones está débilmente acoplado, en que ningunas de ellas se pueden restablecer sin una dependencia en los elementos de la sesión de la capa anterior:

1. El TCP o el UDP vuelve a conectar [la capa OSI 3]
2. TLS, DTL, o IPSec (IKE+ESP) [la capa OSI 4] - reanudación de TLS no se soporta.
3. VPN [capa OSI 7] - El token de la sesión de VPN se utiliza pues un token de autenticación para restablecer a la sesión de VPN sobre un canal asegurado cuando hay una interrupción. Es un mecanismo propietario que es muy similar, conceptual, a cómo un token del Kerberos o un certificado del cliente se utiliza para la autenticación. El token es único y generado criptográficamente por el centro distribuidor, que contiene el ID de sesión más un payload al azar criptográficamente generado. Se pasa al cliente como parte del establecimiento inicial VPN después de que un canal seguro al centro distribuidor se establezca. Sigue siendo válido para el curso de la vida de la sesión sobre el centro distribuidor, y se salva en la memoria del cliente, que es un proceso privilegiado.
   Consejo: Estas versiones ASA y posterior contienen un token criptográfico más fuerte de la sesión: 9.1(3) y 8.4(7.1)

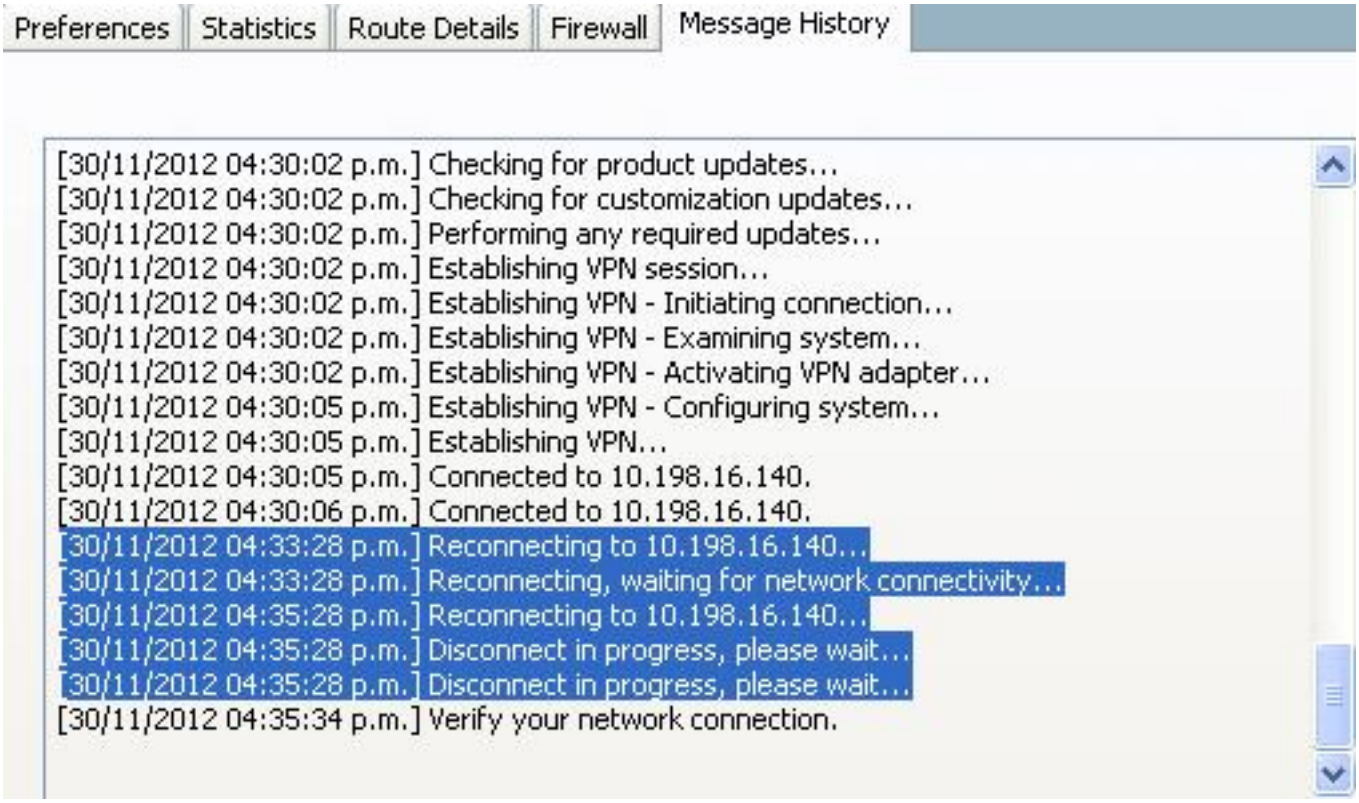
## El proceso real

Se comienza un temporizador del descanso de la desconexión tan pronto como se interrumpa la conexión de red. El cliente de AnyConnect continúa intentando volver a conectar mientras no expire este temporizador. El descanso de la desconexión se fija a la configuración más baja del Ocioso-**descanso de la** directiva del grupo o del **tiempo de conexión máximo**.

El valor de este temporizador se considera en el visor de eventos para la sesión de AnyConnect en la negociación:




En este ejemplo, la sesión debe desconectar después de dos minutos (120 segundos), que se pueden llegar el historial del mensaje del AnyConnect:



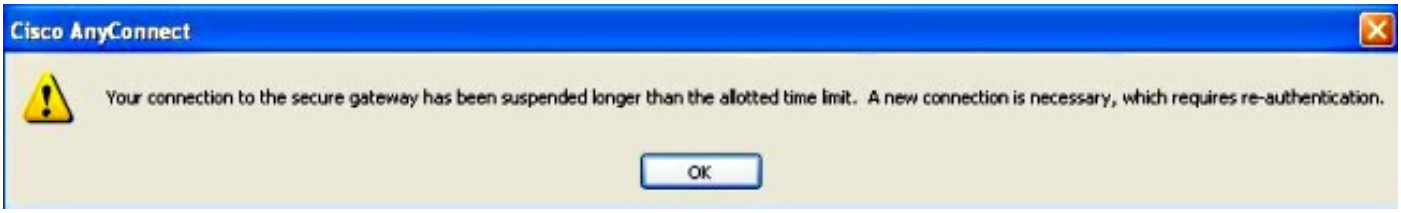

Consejo: Para que el ASA responda a un cliente que esté intentando volver a conectar, la sesión del Padre-túnel debe todavía existir en la base de datos ASA. En caso de Conmutación por falla, los DPD también necesitan ser habilitados para que el comportamiento del volver a conectar trabaje.

Al igual que visible de los mensajes anteriores, el volver a conectar fallado. Sin embargo, si el volver a conectar es acertado, aquí es qué sucede:

1. El Padre-túnel sigue siendo lo mismo; esto no se renegocia porque este túnel mantiene el token de la sesión que se requiere para la sesión para volver a conectar.
2. Se generan las nuevas sesiones SSL y DTL, y los puertos de las diferentes fuentes se utilizan en el volver a conectar.
3. Se restablecen todos los valores de agotamiento del tiempo inactivos.
4. Se restablece el tiempo de espera de inactividad.

Precaución: Sea consciente del Id. de bug Cisco CSCtg33110. La base de datos de la sesión de VPN no pone al día al IP Address público en la base de datos de la sesión ASA cuando AnyConnect vuelve a conectar.

En esta situación donde las tentativas de volver a conectar el fall, usted encuentran este mensaje:




Nota: Este pedido de mejora se ha clasifiado para hacer este más granular: Id. de bug Cisco CSCsl52873 - El ASA no tiene un descanso disconnected configurable para AnyConnect.

# El comportamiento del cliente de AnyConnect en caso del sistema suspende

Hay una característica de itinerancia que permite que AnyConnect vuelva a conectar después de que un sueño PC. El cliente continúa intentando hasta la marcha lenta o los tiempos de espera de la sesión expiran y el cliente no derriba inmediatamente el túnel cuando el sistema entra hiberna/recurso seguro. Para los clientes que no quieren esta característica, fije el tiempo de espera de la sesión a un valor bajo para prevenir el sueño/el curriculum vitae vuelve a conectar.

> Nota: Después de que el arreglo del Id. de bug Cisco CSCso17627 (versión 2.3(111)+), un botón de control fuera introducido para inhabilitar esto vuelva a conectar en la característica del curriculum vitae.

El comportamiento del Auto-volver a conectar para AnyConnect puede ser controlado con el perfil de AnyConnect XML con esta configuración:

```
ASA5520-C# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : walter Index : 1336
Public IP : 172.16.250.17
Protocol : AnyConnect-Parent    <- Here just the AnyConnect-Parent is active
but not SSL-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none
Hashing : AnyConnect-Parent: (1)none
Bytes Tx : 12917 Bytes Rx : 1187
Pkts Tx : 14 Pkts Rx : 7
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : My-Network Tunnel Group : My-Network
Login Time : 17:42:56 UTC Sat Nov 17 2012
Duration : 0h:09m:14s
Inactivity   : 0h:01m:06s           <- So the session is considered Inactive
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
```

Con este cambio, AnyConnect intentará volver a conectar cuando el ordenador se trae detrás del sueño. Los valores por defecto de la preferencia de AutoReconnectBehavior a DisconnectOnSuspend. Este comportamiento es diferente del de la versión de cliente 2.2 de AnyConnect. Para vuelva a conectar después del curriculum vitae, el administrador de la red debe fijar ReconnectAfterResume en el perfil o hacer usuario de las preferencias de AutoReconnect y de AutoReconnectBehavior controlable en el perfil para permitir que los usuarios lo fijen.

# Preguntas Frecuentes

## Q1. ¿Anyconnect DPD tiene un intervalo pero ningunas recomprobaciones - cuántos paquetes tiene que faltar antes de que marque el extremo remoto como muerto?

**R.** Tiene que faltar tres recomprobaciones/cuatro paquetes.

## Q2. ¿Es el proceso DPD diferente para AnyConnect con IKEv2?

**R.** Sí, IKEv2 tiene un número fijo de recomprobaciones - seis recomprobaciones/siete paquetes.

## Q3. ¿Hay otro propósito para el Padre-túnel de AnyConnect?

**A.** Además de ser una asignación en el ASA, el túnel del padre se utiliza para avanzar las actualizaciones de la imagen de AnyConnect del ASA al cliente, porque el cliente no está conectado activamente durante el proceso de actualización.

## Q4. ¿Puede usted filtrar y terminar una sesión apenas a las sesiones inactivas?

**R.** Usted puede filtrar a las sesiones inactivas con el comando **inactivo del filtro del anyconnect de VPN-sessiondb de la demostración**. Sin embargo, no hay comando de terminar una sesión apenas a las sesiones inactivas. En lugar, usted necesita terminar una sesión las sesiones específicas o terminar una sesión todas las sesiones por el usuario (índice - nombre), el protocolo, o el grupo de túnel. Un pedido de mejora, el Id. de bug Cisco CSCuh55707, se ha clasifiado para agregar la opción para terminar una sesión apenas a las sesiones inactivas.

## Q5. ¿Qué sucede al Padre-túnel cuando expira el Ocioso-descanso de los túneles DTL o de TLS?

**R.** La “marcha lenta” al temporizador izquierdo de la sesión del AnyConnect-padre se reajusta después de que se derribe el SSL-túnel o el DTL-túnel. Esto permite que el “ocioso-descanso” actúe como “desconectó” el descanso. Ésta se convierte en con eficacia la época permisible para que el cliente vuelva a conectar. Si el cliente no vuelve a conectar dentro del temporizador, después el Padre-túnel será terminado.

## Q6. ¿Cuál es la punta de guardar la sesión que los temporizadores DPD han desconectado una vez la sesión y porqué el ASA no liberan la dirección IP?

**R.** El centro distribuidor no tiene ningún conocimiento del estado de cliente. En este caso, las esperas ASA para que el cliente esperanzadamente vuelva a conectar hasta los tiempos de la sesión hacia fuera sobre el temporizador de inactividad. El DPD no mata a una sesión de AnyConnect; mata simplemente al túnel (dentro de esa sesión) de modo que el cliente pueda restablecer el túnel. Si el cliente no restablece un túnel, sigue habiendo la sesión hasta que expire el temporizador de inactividad.

Si la preocupación está sobre las sesiones que son consumidas, fije los simultáneo-logines a un valor bajo tal como uno. Con esta configuración, usuarios que tienen una sesión en la base de datos de la sesión tener su sesión anterior borrada cuando inician sesión otra vez.

## Q7. ¿Cuál es el comportamiento si el ASA falla encima de activo al recurso seguro?

**R.** Inicialmente, cuando se establece la sesión, los tres túneles (padre, SSL, y DTL) se replican a la unidad en espera; una vez que el ASA falla encima, se restablecen los DTL y las sesiones de TLS pues no se sincronizan a la unidad en espera, pero cualquier dato atraviesa los túneles debe trabajar sin la interrupción después de que se restablezca la sesión de AnyConnect.

Las sesiones SSL/DTLS no son stateful, así que el estado y el número de secuencia SSL no se mantienen y pueden gravar muy. Así, esas sesiones necesitan ser restablecidas desde el principio, que se hace con la sesión del padre y el token de la sesión.

> Consejo: En caso de evento de falla, las sesiones de cliente VPN SSL no se transportan al dispositivo en espera si se inhabilita el Keepalives.

## Q8. ¿Por qué hay dos diversos descansos, el tiempo de inactividad y el descanso disconnected, si son ambas el mismo valor?

**R.** Cuando los protocolos fueron desarrollados, dos diversos descansos fueron proporcionados para:

- Tiempo de inactividad - El tiempo de inactividad está para cuando no se pasa ningunos datos sobre una conexión.
- Descanso disconnected - El descanso disconnected está para cuando usted abandona a la sesión de VPN porque la conexión se ha perdido y no puede ser restablecida.

El descanso disconnected nunca fue implementado en el ASA. En lugar, el ASA envía el valor de agotamiento del tiempo inactivo para los descansos ociosos y disconnected al cliente.

El cliente no utiliza el tiempo de inactividad, porque el ASA maneja el tiempo de inactividad. El cliente utiliza el valor de agotamiento del tiempo disconnected, que es lo mismo que el valor de agotamiento del tiempo inactivo, para saber cuándo abandonar vuelve a conectar las tentativas puesto que el ASA habrá caído la sesión.

Mientras que está conectado no activamente con el cliente, el ASA descanso la sesión vía el tiempo de inactividad. La razón primaria para no implementar el descanso disconnected en el ASA era evitar la adición de otro temporizador para cada sesión de VPN y el aumento en los gastos indirectos en el ASA (aunque el mismo temporizador se podría utilizar en ambos casos, apenas con diversos valores de agotamiento del tiempo, puesto que los dos casos están mutuamente - exclusiva).

El único de valor añadido con el descanso disconnected es permitir que un administrador especifique un diverso descanso para cuando el cliente no está conectado activamente contra la marcha lenta. Según lo observado anterior, el Id. de bug Cisco CSCsl52873 se ha clasifiado para esto.

## Q9. ¿Qué sucede cuando se suspende la máquina del cliente?

**A.** Por abandono, AnyConnect intenta restablecer una conexión VPN cuando usted pierde la Conectividad. No intenta restablecer una conexión VPN después de que un sistema reanude por abandono. Refiera al cliente de AnyConnect que el comportamiento en caso del sistema suspende para los detalles.

## Q10. ¿Cuando sucede un volver a conectar, el adaptador virtual de AnyConnect agita o hace el cambio de la tabla de ruteo en absoluto?

**R.** Un túnel-nivel vuelve a conectar no hará tampoco. Esto es un volver a conectar en apenas el SSL o los DTL. Éstos van cerca de 30 segundos antes de que abandonan. Si los DTL fallan, apenas se cae. Si el SSL falla, causa un sesión-nivel vuelve a conectar. Un sesión-nivel vuelve a conectar hará de nuevo totalmente la encaminamiento. Si la dirección cliente asignada en el volver a conectar, o ninguna otra parámetros de la configuración que afectan el adaptador virtual (VA), no ha cambiado, después el VA no se inhabilita. Mientras que es inverosímil tener cualquier cambio en los parámetros de la configuración recibidos del ASA, es posible que un cambio en la interfaz física usada para la conexión VPN (por ejemplo, si usted descola y va de atado con alambre a WiFi) podría dar lugar a un diverso valor de la Unidad máxima de transmisión (MTU) (MTU) para la conexión VPN. El valor MTU afecta el VA, y un cambio a él hace el VA ser inhabilitado y después ser vuelto a permitir.

## Q11. ¿Hace? ¿El auto vuelve a conectar? ¿proporcione la Persistencia de sesión? ¿Si es así hay funcionalidad extra agregada en el cliente de AnyConnect?

**A.** AnyConnect no proporciona ninguna “magia adicional” para acomodar la Persistencia de sesión para las aplicaciones. Pero la conectividad VPN se restablece automáticamente poco después de que conectividad de red a los curriculums vitae seguros del gateway, con tal que no hayan expirado la marcha lenta y los tiempos de espera de la sesión configurados en el ASA. Y a diferencia del cliente IPSec, el automáticos vuelven a conectar los resultados en el mismo dirección IP del cliente. Mientras que AnyConnect intenta volver a conectar, el adaptador virtual de AnyConnect sigue siendo habilitado y en el estado conectado, así que el dirección IP del cliente sigue siendo presente y habilitado en PC del cliente el tiempo entero, que da la persistencia del dirección IP del cliente. PC del cliente las aplicaciones, sin embargo, todavía percibirán probablemente la pérdida de conectividad a sus servidores en la red para empresas si dura demasiado para que la conectividad VPN sea restablecida.

## Q12. Esta característica trabaja en todas las variantes de Microsoft Windows (Vista de 32 bits y 64-bit, XP). ¿Cómo sobre Macintosh? ¿Trabaja en OS X 10.4?

**R.** Esta característica trabaja en el mac y Linux. Ha habido problemas con el mac y Linux, pero mejoras recientes se han llevado a cabo, determinado para el mac. Linux todavía requiere un poco de soporte adicional (CSCsr16670, CSCsm69213), pero la funcionalidad básica está allí también. En lo que respecta a Linux, AnyConnect no reconocerá que ha ocurrido un suspender/un curriculum vitae (sueño/estela). Esto tiene básicamente dos impactos:

- El perfil/la configuración de preferencias de AutoReconnectBehavior no se puede soportar en Linux fuera suspende/el soporte del curriculum vitae, así que un volver a conectar ocurrirá siempre después de que suspenda/curriculum vitae.
- En Microsoft Windows y Macintosh, vuelve a conectar se realizan inmediatamente en la sesión llana después del curriculum vitae, que permite un Switch más rápido a una diversa interfaz física. En Linux, porque AnyConnect está totalmente inconsciente del suspender/del curriculum vitae, vuelve a conectar ocurrirá en el túnel-nivel primero (SSL y DTL) y esto pudo significar que vuelve a conectar la toma levemente más de largo. Pero vuelve a conectar

todavía ocurrirá en Linux.

## Q13. ¿Hay limitaciones a la característica en términos de Conectividad (atada con alambre, Wi-fi, 3G y así sucesivamente)? ¿Soporta la transición a partir de un modo a otro (del Wi-Fi a 3G, a 3G a atado con alambre, y así sucesivamente)?

No atan a **A.** AnyConnect a una interfaz física determinada para la vida de la conexión VPN. Si la interfaz física usada para la conexión VPN se pierde o si vuelva a conectar las tentativas sobre ella exceden cierto umbral del error, después AnyConnect utilizará no más esa interfaz e intentar alcanzar el gateway seguro con cualesquiera interfaces están disponibles hasta la marcha lenta o los temporizadores de sesión expire. Observe que un cambio en la interfaz física podría dar lugar a un diverso valor MTU para el VA, que hará el VA tener que ser inhabilitado y ser vuelto a permitir, pero aún con el mismo dirección IP del cliente.

Si hay alguna interrupción del funcionamiento de la red (interfaz abajo, redes cambiadas, interfaces cambiadas), AnyConnect intentará volver a conectar; no se necesita ninguna reautentificación encendido para volver a conectar. Esto incluso se aplica a un Switch de las interfaces físicas:

Ejemplo:

```
ASA5520-C# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : walter Index : 1336
Public IP : 172.16.250.17
Protocol : AnyConnect-Parent    <- Here just the AnyConnect-Parent is active
but not SSL-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none
Hashing : AnyConnect-Parent: (1)none
Bytes Tx : 12917 Bytes Rx : 1187
Pkts Tx : 14 Pkts Rx : 7
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : My-Network Tunnel Group : My-Network
Login Time : 17:42:56 UTC Sat Nov 17 2012
Duration : 0h:09m:14s
Inactivity   : 0h:01m:06s          <- So the session is considered Inactive
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
```

## Q14. ¿Cómo se autentica la operación del curriculum vitae?

**R.** En un curriculum vitae, usted resomete el token autenticado que permanecerá para el curso de la vida de la sesión, y la sesión entonces se restablece.

## Q15. ¿La autorización LDAP también se realiza sobre vuelve a conectar o solamente la autenticación?

**R.** Esto se realiza solamente en la conexión inicial.

### Q16. ¿El pre-login y/o el funcionamiento hostscan sobre reanuda?

**R.** No, éstos ejecutados en la conexión inicial solamente. Algo similar slated para la característica periódica futura de la evaluación de la postura.

### Q17. ¿En cuanto al Equilibrio de carga VPN (LB) y al curriculum vitae de la conexión, el cliente conectará detrás directamente con el miembro de clúster que fue conectado con antes?

**R:** Sí, esto está correcto puesto que usted no lo hace re-resolución el nombre de host vía el DNS para re-estblishment de una sesión existente.

## Información Relacionada

- Referencia ASA DPD: Id. de bug Cisco CSCsr63074 - DPD no enviado cuando el par es muerto y túnel no ocioso en s2s con 7.2.4
- Soporte Técnico y Documentación - Cisco Systems